VPNremote for 46xx Series IP Telephone Installation and Deployment Guide.

June 28th 2006

1 Table of Contents

1 TABLE OF CONTENTS 2

2 INTRODUCTION 4

3 PREPARING SECURITY GATEWAY FOR REMOTE ACCESS 4

3.1 IKE AND IPSEC CONFIGURATION 5
3.2 CLIENT IP ADDRESS POOL – ALL SGS 6
3.3 DNS SERVER – ALL SGS 7
3.4 PROTECTED IP SUBNETS – ALL SGS 7
3.5 WELCOME BANNER 8
3.6 REAUTHENTICATION ON REKEY 8
3.7 FIREWALL RULES ON THE PRIVATE SIDE OF THE SECURITY GATEWAY 9
3.8 FIREWALL RULES ON THE PUBLIC SIDE OF THE SECURITY GATEWAY 10
3.9 MANUFACTURER SPECIFIC ISSUES 10
3.10 VPNREMOTE PHONE LOAD DISTRIBUTION AND FAILOVER 11

4 ADMINISTRATION DIFFERENCES OF VPNPHONES 11

4.1 SCRIPT FILES 12
4.2 DHCP SERVER 12
4.3 FILE SERVER 13

5 PREPARING FILE SERVER FOR INSTALLING VPNREMOTE 13

5.1 VPNREMOTE SOFTWARE BUNDLE FOR 4600 SERIES IP TELEPHONE 13
5.2 COLLECTING INFORMATION REQUIRED FOR MODIFYING SCRIPT FILES PROVIDED WITH VPNREMOTE SOFTWARE BUNDLES 14
5.3 CREATING 46VPNSETTING.TXT 14
5.4 COPYING FILES ON FILE SERVER 15

6 INSTALLING VPNREMOTE 15

7 BATCH INSTALLING VPNPHONE 16

7.1 STEP #1 17

7.2 STEP #2 17
7.3 STEP #3 17
7.4 STEP #4 17
7.5 STEP #5 17
7.6 STEP #6 17

8 DEPLOYING VPNPHONE AT REMOTE LOCATION 17

8.1 TESTING IPSEC TUNNEL QUALITY 17
8.2 FIREWALL RULES ON THE SOHO FIREWALL 18

9 USING ONE TIME PASSWORD SCHEME 19

10 INSTALLING LICENSE SERVER 19

10.1 SUPPORTED PLATFORMS 19
10.2 WEBLM INSTALLATION 19
10.3 CONFIGURATION 20
10.4 VPNREMOTE PHONE SYSLOG MESSAGES 20
10.5 VPNREMOTE PHONE LICENSE 22

11 PREPARING COMMUNICATION MANAGER FOR VPNREMOTE PHONE 22

12 FREQUENTLY ASKED QUESTION 23

12.1 HOW DO I KNOW IF VPNREMOTE PHONE WILL WORK WITH MY SECURITY GATEWAY? 23
12.2 DOES VPNREMOTE PHONE SUPPORT AUTHENTICATION USING SECUREID FROM RSA? 24
12.3 WHAT ARE SPECIAL CONSIDERATION REQUIRED WHEN USING SECUREID FROM RSA FOR AUTHENTICATING VPNREMOTE PHONE USERS ? 24
12.4 HOW IS THE PRESHARED KEY AND PASSWORD STORED BY VPNREMOTE PHONES? .. 24
12.5 MY SOHO ROUTER SUPPORTS QOS, HOW DO I USE IT FOR VPNREMOTE PHONES? .. 24
12.6 TALK PATH DOES NOT ESTABLISH WHEN CALLING SOME EXTENSIONS? 25
12.7 HOW DOES THE WEBLM SERVER INTERACT WITH THE VPNPHONE 25

2 Introduction

This document describes how to install VPNremote firmware on 4600 series IP Telephone product line. The 4600 Product line of IP Telephone consist of multiple models; not all of which have the capability to support VPNremote firmware. The table below lists all the 4600 series IP telephone models and indicates those which will support VPNremote firmware.

IP Telephone Model	VPNremote supported
4601	No
4602	No
4602SW	No
4610SW	Yes
4620	No
4620SW	Yes
4621SW	Yes
4622SW	Yes
4625SW	Yes
4630	No
4630SW	No
4690SW	No

3 Preparing Security Gateway for Remote Access

To create a successful VPN tunnel, the VPNremote phone must be capable of setting up IPsec tunnel between itself and a Security Gateway. The VPN phone can use any of the methods discussed below depending upon the type of security gateway used:

1. **Avaya Security Gateway**: When the VPNremote phone establishes a TLS session with an Avaya security gateway (VSU or SG) it uses the Avaya Proprietary CCD protocol. During the TLS handshake portion of the CCD protocol, the phone verifies that the certificate presented by the security gateway is issued by a trusted Avaya Certificate Authority (CA). The next phase involves the exchange of user credentials. After that user credential are sent to the security gateway, if user credentials are correct, the security gateway sends the IKE configuration necessary for establishing IPsec SAs, an IP address from the Client IP Address pool, the IP address of the DNS server, a List of protected IP Subnets and the Welcome Banner. This set of information is sufficient to create the VPN tunnel and to allow the IP phone code to communicate with its CM to become operational.

2. **Third Party Security Gateways using Xauth with Preshared Key**: The VPN Phone will communicate with any third party security gateway that strictly implements the Xauth with preshared key. IKE Extended Authentication (Xauth) is a draft RFC developed by Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. Xauth allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. The VPNphone uses the preshared key to authenticate the security gateway and create a temporary secure path to allow the end user to present credentials to the gateway. After user authentication is successful, the security gateway sends an IP address from the Client IP Address pool, IP address of the DNS server and the Welcome Banner. The VPN Phone has been tested with the implementation of Xauth with preshared key implemented by Cisco and Juniper security gateways; however, any security gateway that process Xauth with PSK exactly like the juniper or Cisco gateway should work with the VPNphone.

All of the supported security gateways have several options and must be configured to support the creation of a VPN tunnel with the VPNphone. To support the VPNphone, the administrator of the security gateway must prepare the security gateway for remote access using one of the methods mentioned above. Refer manufacturer provided admin guide for all the procedures necessary to configure the gateway.

To verify the configuration steps you can use the manufacturer provided IPsec Client to setup a VPN tunnel using the protocol selected. If the VPN tunnel is successfully established, you have verified that the security gateway is correctly configured and the step of creating a VPN tunnel between the VPNphone and the security gateway should be successful.

The remainder of this section will provide the needed sets of capabilities that must be configured into the security gateway to support successful interactions between the gateway and the phone. Each of the paragraphs describes the most common of these VPN Configuration parameters and there relevance to VPNremote phones as IPsec clients.

3.1 IKE and IPsec Configuration

4.1.1 Avaya Proprietary CCD protocol

All the necessary interactions between the VPNphone and an Avaya security gateway are handled using default configurations; therefore, no actions must be taken with respect to the security gateway.

4.1.2 Xauth with Preshared Key method

By default VPNremote phones sends following proposal list during phase1 negotiation, so the security gateway should be configured to accept one of these IKE parameters:

1. AES-128,HMAC-SHA1,DH-2
2. AES-128,HMAC-MD5,DH-2
3. 3DES,HMAC-SHA1,DH-2

4. 3DES,HMAC-MD5,DH-2
5. DES,HMAC-SHA1,DH-2
6. DES,HMAC-MD5,DH-2
7. AES-192,HMAC-SHA1,DH-2
8. AES-192,HMAC-MD5,DH-2
9. AES-256,HMAC-SHA1,DH-2
10. AES-256,HMAC-MD5,DH-2

By default VPNremote phone sends following proposal list during phase 2 negotiation

1. ESP,AES-128,HMAC-SHA1,DH-None
2. ESP,AES-128,HMAC-MD5,DH-None
3. ESP,3DES,HMAC-SHA1,DH- None
4. ESP,3DES,HMAC-MD5,DH- None
5. ESP,DES,HMAC-SHA1,DH- None
6. ESP,DES,HMAC-MD5,DH- None
7. ESP,AES-192,HMAC-SHA1,DH- None
8. ESP,AES-192,HMAC-MD5,DH- None
9. ESP,AES-256,HMAC-SHA1,DH- None
10. ESP,AES-256,HMAC-MD5,DH- None

Refer to NVIKEDHGRP, NVPFSDHGRP, NVIKEP1ENCALG, NVIKEP2ENCALG, NVIKEP1AUTHALG and NVIKEP2AUTHALG system variable description in the accompanying 46vpnsetting_readme.txt on how to modify the list of proposals sent by VPNremote phones.

4.1.3 Security Association lifetime

VPNremote always proposes security association life time of 1 day. This value cannot be modified in the phone; However, if the security gateway is configured to offer a different life time, the VPNremote phone will accept the life time offered by the SG. It is recommended that you always configure security gateway with security association life time of 5 days in order to minimize the complex calculations required by a re-key transaction.

4.1.4 Avaya proprietary CCD SA lifetime

VPNremote phone uses IKE and IPsec configuration sent by the security gateway. Hence no special consideration or customization required on VPNremote phones. For Avaya security gateway it is recommended to use IKE and IPsec SA life time of 8 hours instead of 5 days as recommended for non-Avaya security gateways.

3.2 Client IP Address Pool – All SGs

The client IP address pool is the IP address range configured on the security gateway for IPsec clients. VPNremote phone uses an address from the pool as its address for communicating with hosts on the private side of the security gateway. Size of the Client IP Address Pool determines the maximum number of IPsec clients that can connect to the security gateway at any time. Limit the size of client IP address pool to restrict the

number of IPsec clients that can connect to a security gateway. See 4.10 for details regarding Load Distribution and failover.

3.3 DNS server – All SGs

Security Gateways are capable of delivering IP address of the DNS server located on the private (protected) side of the security gateway to the IPsec clients. If you are planning to make use of DNS names for host on the private side of the security gateway, make sure that the security gateway is configured to deliver DNS server IP addresses to the IPsec clients.

Some security gateways are capable of delivering default domain prefix to the IPsec clients, but the **VPNremote phone ignores the default domain prefix sent by the security gateway; therefore, the SG must always send use fully qualified domain names.**

3.4 Protected IP Subnets – All SGs

Security Gateways provide a mechanism to specify the IP subnets accessible to the IPsec clients. It is highly recommended that you configure all zeros as the IP subnets accessible to the IPsec clients. If you choose to ignore this advice make sure that you have covered all the IP subnets required for proper functioning of IP telephone, failure to do so will result in unexpected results.

3.4.1 Performance consideration

An IPsec SA is created for each protected IP subnets. Thus if you configure 5 protected IP subnets and there are 200 VPNremote phones, Security Gateway will have to maintain 1000 IPsec SAs instead of just 200 in case if you had all zeros as IP subnets. Since the table must be linearly searched, keeping the table small enhances performance considerably.

Most security gateway manufacturer's published performance numbers assume that each IPsec client builds only 1 SA.

4.4.1.1 Alternative approach

Use firewall rules on the private side of the security gateway to prevent IPsec clients from sending and receiving traffic to and from protected IP subnets.

4.4.1.2 Xauth with Preshared Key method

IPsec client must be manually configured with the list of IP subnets protected by Security Gateway. By default VPNremote phone uses all zeros as the IP subnet protected by the Security Gateway. Maximum number of protected IP subnets that can be configured on VPNremote phones is limited to 5. Refer to the description of NVIPSECSUBNET in the accompanying 46vpnsetting_readme.txt for more details.

4.4.1.3 Avaya proprietary method

VPNremote phone uses protected IP subnets list sent by security gateway hence modifying 46vpnsetting.txt is not required even if you are not using all zero as protected IP subnets. However it is still recommended to use all zero as the protected IP subnets.

3.5 Welcome Banner

Many security gateways provide mechanism to deliver a Welcome Banner containing any arbitrary text. The welcome Banner (or in the case of the Avaya SG client legal message) can be used to deliver script text to the VPNphone when the VPN is being established. Configuration parameters or changes to configuration parameters that are the same for all VPNphones can be delivered using this scripting method.
The script portion of the banner message is indicated by the <START_SCRIPT> and <END_SCRIPT> commands. Any text after the script is delivered as a welcome banner. Within the script commands that would appear in the 46XX_settings.txt file can be delivered. For example

```
<SCRIPT_START>

SET MCIPADD callserver.intranet.com
SET TFTPSRVR myfserver.intranet.com
SET TFTPDIR path

<SCRIPT_END>
```

The script start and end markers are case sensitive.
If script start and end markers are not present in the Welcome Banner, VPNremote phones ignore it.

4.5.1 Avaya proprietary CCD method

Welcome banner is referred to as “Client Legal Message”. It sent to the IPsec clients prior to user authentication hence it is advised that you don’t use this for sending information that you consider sensitive. For example use DNS names instead of actual IP address otherwise a potential intruder who may be randomly scanning for applications that could be attacked may discover an IP address of the DNS server within the protected network.

4.5.2 Xauth with preshared key method

At the present time, the only SG known to support welcome banner is Cisco VPN 3000 series concentrator. This device sends the Welcome banner only after validating user credential; hence you can put any information in the welcome banner that you are willing to share with VPNremote phone users.

3.6 Reauthentication on ReKey

This setting is specific to Xauth with Preshared key method. It is highly recommended that you disable Reauthentication on Rekey if VPNphones are configured to prompt for password every time rekey is required or when using token based authentication. If reauthentication on rekey is used, the VPNphone will become disconnected from the

internal network until reauthentication takes place and during that period, the phone will not receive any calls. Refer to the description of NVVPNPSWDTYPE in the accompanying 46vpnsetting_readme.txt file.

3.7 Firewall rules on the private side of the security gateway

It is recommended that VPNremote phones be given the same level of access to the enterprise network as the phones inside the enterprise network. If this is not feasible use the port and protocol usage table below for creating firewall rules on the private side of the security gateway.

Source	Range	Config-urable source	protoc ol	Destination	Dest Range	Configura ble dest	Response from dest
Phone	1500-6500	No	TCP	Call Server	1720	No	Yes
Phone	49300-65535	No	UDP RAS	Call Server	1719	No	Yes
Phone	2048-3028	Yes	UDP RTP	Various	2048-3028	Yes	No
Various	2048-3028	Yes	UDP RTP	Phone	2048-3028	Yes	No
Phone	2049-3027	Yes	UDP RTCP	AIM Server	5005	Yes	No
Phone	1024-65535	No	UDP TFTP	TFTP Server	69	No	Yes
TFTP Server	1024-65535	No	UDP TFTP	Phone	1024-65535	No	Yes
Phone	1024-65535	No	TCP HTTP	HTTP Server	80	Yes	Yes
Phone	1024-65535	No	TCP TLS	TLS Server	443	Yes	Yes
Phone	1024-65535	No	TCP HTTP	WebLM Server	8080	Yes	Yes
SNMP Station	1024-65535	No	UDP SNMP	Phone	161	No	Yes
Phone	1024-65535	No	UDP DNS	DNS Server	53	No	Yes
Phone	1024-65535	No	UDP Syslog	Log server	514	No	No

Phone	1645	No	UDP QTEST	Phone	1645	No	No

3.8 Firewall rules on the public side of the security gateway

Use the table below to create firewall rules on the public side of the security gateway

Source	Source Range	Config-urable source	protocol	Destination	Dest Range	Configura ble dest	Response from dest
Phone	Any	No	TCP TLS	SG public interface	1443	No	Yes
Phone	Any	No	UDP IKE / IPsec	SG public interface	500	No	Yes
Phone	Any	No	UDP IKE / IPsec	SG public interface	4500	No	Yes
Phone	NA	NA	ESP (51)	SG public interface	NA	NA	NA

3.9 Manufacturer specific issues

This section highlights the known manufacturer specific issues which interfere with VPNremote phones functionality.

3.9.1 Cisco systems, Inc. VPN 3000 series concentrator

1. Under Client FW tab of the VPNremote phone group “No Firewall” option must be selected for the attribute “Firewall Setting”.
2. Under HW Client tab of the VPNremote phone group, all attributes must be left unchecked.
3. Under NAC tab of the VPNremote phone group “Enable NAC” must be left unchecked.
4. Under IPsec tab of the VPNremote phone group, the value for attribute“Client type & Version limiting” must be left blank.
5. VPNremote phones users will not be able to change password upon password expiry when using Radius with expiry.

4.9.1.1 Symptoms:

In case of 1,2,3 and 4 VPNremote phone will fail to complete IKE phase 2.
In case of 5 authentication failure after password expiry.

3.9.2 Juniper/Netscreen

1. Security Gateway must be running Screen OS 5.1.0 or higher.
2. Disable H.323 ALG unless the gateway has patch XXXX installed.
3. Disable shuffling on Call Server.

4.9.2.1 Symptoms:

In case of 1 and 2 VPNremote phone will not encounter any errors during tunnel setup but will fail to register with the call server on 4620, 4621, 4622 and 4610 models and there will not be any dial tone on 4625 models.
In the case of 3 VPNremote phones will fail to establish talk path.

3.10 VPNremote Phone Load Distribution and Failover

VPNphones can be configured with the fully qualified domain name (FQDN) of the security gateway instead of actual IP address. Use DNS Name Server Load Balancing feature and size of the Client IP address pool to uniformly distribute VPNphones across multiple security gateways.

Example: How to evenly distribute 500 VPNremote phones on 5 security gateways such that if one of the security gateway goes down there are no more than 125 VPNremote phones on one security gateway.

1. Configure DNS server to return security gateway IP addresses in a round robin fashion. The DNS server returns all IP addresses in response to a DNS query but keeps changing the order of the list which means each subsequent VPNphone will get a different one of the 5 IP addresses.
2. Limit the size of Client IP address pool to 125 on each security gateway. Initially when all security gateways are available there will be 100 VPNremote phones on each security gateway. If one of the security gateway goes down for some reason, all 100 VPNremote phones connected to that security gateway will reboot in approximately 6 minutes and redistribute evenly among remaining 4 security gateways because of the limit on Client IP address pool.
3. Let's see what would have happened if you had not imposed limit of 125 on Client IP address pool. Say the 5 security gateways are A, B, C, D and E. DNS server is rotating this list after every DNS query. Now C goes down. All VPNphones connected to C will reboot and D will end up absorbing 40 VPNphones from C while A, B and E will absorb only 20 VPNphones from C because of the lack of limit on Client IP address pool.

Caution: The example above assumes that none of the VPNphones in the system terminated abnormally. However this is far from true. Every time a VPNphone restarts without gracefully shutting down the previous session it might end up consuming two addresses from the cumulative client IP address pool. For example if a phone was connected to A but restarted due to power failure and next time it got connected to B. This phone has now consumed an additional IP address from cumulative IP address pool. As a rule of thumb always keep the cumulative size of IP address pool 15% more than the number of VPNphones.

4 Administration Differences of VPNphones

This section highlights the differences between administration of VPNphones and non-VPNremote phones within the enterprise network.

4.1 Script Files

At startup all IP telephones download script files from the file server.
VPNphones download following script files from file server in the order given below:

1. 46vpnupgrade.scr
2. 46vpnsetting.txt
3. 46xxsettings.txt

non-VPNphones download following script files from file server in the order given below:

1. 46xxupgrade.scr
2. 46xxsettings.txt

This arrangement has been provided so that you can administer:

1. All options specific to IP telephone functionality in 46xxsettings.txt.
2. All options specific to VPNremote phones in 46vpnsetting.txt.
3. Upgrade/Downgrade VPNremote phones through 46vpnugrade.scr and non-VPNremote phones through 46xxupgrade.scr

While maintaining a single file server for both VPN and non-VPN phones.

4.2 DHCP Server

It is a common practice for an administrator to use the DHCP server within the enterprise network for delivering following set of information to the 4600 series IP telephones within the enterprise

1. IP address of the phone.
2. IP address of the DNS server.
3. Subnet mask.
4. IP address of the default gateway.
5. Default domain prefix.
6. IP address or DNS name of the call server.
7. IP address or DNS name of the file server.
8. Type of the file server.
9. Directory path on file server.

DHCP is used to reduce the administrative burden associated with manual configuration of Call Server and File server IP addresses on each IP telephone. For VPNphones, it is not feasible to configure items 5 through 9 on the enterprise DHCP server because VPNphone lies outside the trusted network. To fill this void the VPNphone provides the capability to save information 7 through 9 in the phone's nonvolatile memory via 46vpnsetting.txt file (See NVVPNFILESRVR description in the accompanying 46vpnsetting_readme.txt file). Now IP address or DNS name of the call server can be delivered to VPNphones through 46xxsettings.txt or 46vpnsetting.txt by setting MCIPADD variable in the script files.

SET MCIPADD callserver.intranet.com

5.3.1 Using Welcome Banner for VPN phones

If supported by the security gateway, you can use the welcome banner (or client legal message) to deliver items 5 through 9 at phone at startup thus eliminating dependency on a File Server.

Example:

Call Server IP address	mycocallsrvr
File Server IP address	mycofsrvr
File Server Path	phone
Domain	mycompany.com
File server type	TFTP

Insert following lines into the Welcome Banner

```
<SCRIPT_START>
SET MCIPADD mycocallsrvr
SET TFTPSRVR mycofsrvr
SET TFTPDIR phone
SET DOMAIN mycompany.com
<SCRIPT_END>
```

Caution: Welcome Banner (Client Legal Message) configured on Avaya Security Gateway is visible to the whole world. Avoid placing sensitive information in the Welcome Banner if using Avaya Security Gateways.

4.3 File Server

Due to the limitation mentioned in previous section, VPNphones require that the file server always be available at startup to provide voice service to the VPNphone user. This is different from phones within the enterprise which continue to provide basic voice services even if the file server was down at startup.

5 Preparing File Server for Installing VPNremote

This section assumes that your enterprise network is already setup and prepared for installing and upgrading software for 4600 Series IP Telephone.
Refer to “4600 Series IP Telephone LAN Administration Guide 555-233-507” for detailed information regarding procedure for setting up the DHCP server WebLM server, and File servers.

5.1 VPNremote software bundle for 4600 Series IP telephone

VPNremote software package comes in zip format and includes following Application files and script files.

1. 46xxvpn.scr
2. 46vpnupgrade.scr
3. 46vpnsetting_ciscoxauthwithpsk.txt
4. 46vpnsetting_juniperxauthwithpsk.txt

5. 46vpnsetting_avaya.txt
6. Application File(s) for all supported 4600 series IP telephone models.
7. WebLM server application

5.2 Collecting information required for modifying script files provided with VPNremote software bundles

1. Security Gateway Manufacturer
2. IP Address or DNS name of the primary security gateway.
3. IP Address(es) or DNS name(s) of the backup security gateway.
4. IP Address or DNS name of the File Server for VPNremote phones
5. IP Address or DNS name of the License Server
6. Group Name (IKE ID), if using non-Avaya Security Gateway.
7. MAC Address of the first network interface of the intended WebLM server (See WebLM documentation)

Optionally

8. IKE Phase 1 Diffie-Hellman group if you have not configured Group 2 on the Security Gateway.
9. IKE Phase 2 Diffie-Hellman group if you have enabled PFS.
10. IP Address or DNS name of the SNMP management station.
11. SNMP read string.
12. IP Address or DNS name of the Syslog Server.
13. IP Address or DNS name of the Call Server.
14. Default Domain prefix.

5.3 Creating 46vpnsetting.txt

Unzip the content of VPNphone software bundle in a temporary location. Use the table below to select the template file from VPNphone software package for creating 46vpnsetting.txt

Security Gateway Manufacturer	Template for 46vpnsetting.txt
Avaya	46vpnsetting_avaya.txt
Cisco	46vpnsetting_ciscoxauthwithpsk.txt
Juniper/Netscreen	46vpnsetting_jnprxauthwithpsk.txt

After selecting the appropriate template for 46vpnsetting.txt, fill in the required parameters using the information gathered in previous section. The table below shows which information gathered in previous section corresponds to what parameters in the template 46vpnsetting.txt file

Parameter Name from 46vpnsetting	Information serial number from previous section
NVSGIP	2
NVBACKUPSGIP	3

NVVPNFILESRVR	4
NVWEBLMURL	5
NVIKEID	6
NVIKEDHGRP	7
NVPFSDHGRP	8
SNMPADD	9
SNMPSTRING	10
LOGSRVR	11
MCIPADD	12
DOMAIN	13

5.4 Copying files on File Server

Copy the newly created 46vpnsetting.txt file along with other application and script files extracted from VPNphone software bundle into the file server download directory and add following lines at the beginning of the existing 46xxupgrade.scr file.

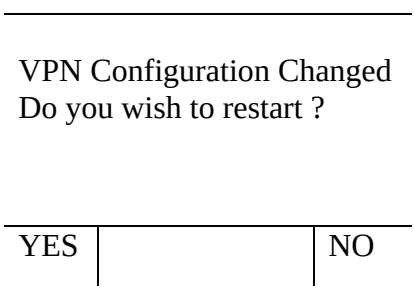
```
IF $GROUP SEQ 876 goto DEFVPN
goto NOVPN

# DEFVPN
GET 46xxvpn.scr
goto END

# NOVPN
```

6 Installing VPNremote

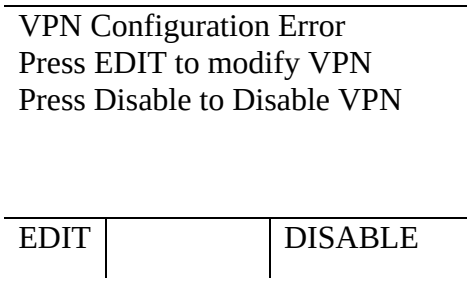
After preparing File Server as described in Section 6, you are ready to start installing VPN firmware on 4600 series IP telephone. To begin the process, simply plug the phone into the enterprise network. Let the phone register with the call server. Once phone is registered modify phone group to 876 and restart the phone by pressing following key sequence

MUTE 4 7 6 8 7 #
8 7 6 # #
MUTE 7 3 7 3 8 # * #

Depending on the speed of your network and existing firmware version on phone it may take up to 5 minutes. The VPNphone is ready for deployment when you see following message on the phone display



This message remains only for 25 seconds after which phone will restart itself hence you might end up seeing this message on the phone display.



This error message means that some information required for setting up the IPsec tunnel is missing. In this case VPNremote phone user must enter the following by pressing the softkey corresponding to <EDIT> label:

1. User Name.
2. Password.
3. Presahred Key if using PSK with Xauth method for setting up the tunnel.

At this stage the VPNphone is ready for deploying at remote location. Refer to XXX for instructions that you must provide to end user for deploying VPNphone at remote location.

7 Batch Installing VPNphone

The procedure described in section 6 to 7 for installing VPN firmware on 4600 series IP telephone requires manually setting each phone's GROUP to 876 hence does not scale well when installing firmware on hundreds of 4600 series IP telephone. To efficiently deploy many VPNphones follow the instructions below:

7.1 STEP #1

Setup the enterprise File Server as described in section 6. This file server will be used by VPNphones when deployed in the remote location.

7.2 STEP #2

Setup a DHCP server and File server in an isolated network as described in “IP Telephone LAN administration guide”

7.3 STEP #3

Now copy the 46vpnsetting.txt file created in section 6.3 along with other application and script files extracted from VPNphone software bundle into the file server download directory of the file server setup in previous STEP.

7.4 STEP #4

Rename the 46xxvpn.scr file present in the download directory to 46xxupgrade.scr.

7.5 STEP #5

Edit 46xxvpnsetting.txt file to include any sensitive information such as preshared key (Xauth method) common to all VPNphone users. This way you can avoid sharing the preshared key with VPNphone users.

7.6 STEP #6

Now plug the 4600 series IP telephone(s) to be configured into the isolated network. Now wait for phones to display messages as described in section 7.

8 Deploying VPNphone at Remote Location

Plug the VPNremote phone into the SOHO network. Wait for phone to display the VPN the configuration error message as described in section 7. Press the EDIT Soft Key and enter following information:

1. VPNremote phone’s User Name.
2. VPNremote phone’s User Password.
3. VPNremote phone’s Group Password (unless it was preconfigured).

Press the Done Soft Key and wait for phone to build IPsec tunnel and register with the call server.

8.1 Testing IPsec Tunnel Quality

The VPNphone has a utility that allows the user to test the quality of the path from the phone through the SOHO network, the ISP, and the Internet to the SG. To invoke the Qtest, press following key sequence:

MUTE 8 7 6 6 6 3 # *

Press the “QTEST” softkey, to bring up the QTEST application screen. In the QTEST application screen press START soft key to start the QTEST and STOP softkey to stop

the QTEST. Following QTEST statistics are displayed on the phone screen while QTEST is running (Use Page Left / Right Keys to scroll between pages).

1. Percent packet lost.
2. Round trip delay of the last packet received.
3. Percent packet late. (RTT was more than 400 ms)
4. Number of packets sent.
5. Number of packets received.
6. Average Round Trip Delay.
7. Maximum Round Trip Delay.
8. Number of packets lost.
9. Size of biggest Burst Lost.
10. Number of packets received out of sequence.
11. Number of interruptions encountered.

If a log server is configured VPNphone sends these statistics to the log server every 5 minutes or when the test is stopped.

8.2 Firewall rules on the SOHO firewall

Use following table to create firewall rules on the SOHO firewall (If applicable) to allow VPNphone to communicate with the security gateway.

Source	Source Range	Config-urable source	protocol	Destination	Dest Range	Configura ble dest	Response from dest
Phone	Any	No	TCP TLS	SG public interface	1443	No	Yes
Phone	2070	No	UDP IKE / IPsec	SG public interface	500	No	Yes
Phone	2070	No	UDP IKE / IPsec	SG public interface	4500	No	Yes
Phone	500	No	UDP IKE / Ipsec	SG public interface	500	No	Yes
Phone	4500	No	UDP IKE / Ipsec	SG public interface	4500	No	Yes
SG public interface	NA	NA	ESP (51)	Phone	NA	NA	NA
Phone	NA	NA	ESP(51)	SG public interface	NA	NA	NA

9 Using One Time Password Scheme

One Time Password scheme refers to authentication mechanisms where a password cannot be reused for example SecureID from RSA inc. Add following line at the very begining of the 46vpnsetting.txt file created in section 6.3

SET NVVPNPSWDTYPE 3

Refer to 46vpnsetting_readme.txt file provided with VPNremote phone software bundle for further details regarding NVVPNPSWDTYPE variable.

10 Installing License Server

10.1 Supported Platforms

Apache-Tomcat versions are: 5.0.28 used with JRE 1.4.2_03
Apache-Tomcat version 5.5.9 used with JRE 1.5.0_02
Apache-Tomcat version 5.5.17 used with JRE 1.5.0_06

10.2 WebLM Installation

Pre-Installation Procedure

This section will describe the set of steps that must be taken before this release is installed.

- Install a valid version of JRE on the machine where WebLM will be deployed. Please ensure to install the correct version as per the operating system (on which WebLM will be running).

- Install the respective version of Apache-Tomcat on the machine where WebLM will be running. Please ensure to install the correct version as per the operating system (on which WebLM will be running).

- Ensure that on the machine on which WebLM will be deployed has an entry for the local host IP address in the hosts file.

E.g. in case of Windows, the file is usually located under C:\WINNT\system32\drivers\etc folder by the name hosts. The entry in this file should look like:

<Localhost_IP_address> <localhost>

E.g. in case of Linux, this file is located under /etc folder by the name hosts. Entry in this file should look something like below:

<Localhost_IP_address> <Machine_Name> <localhost.localdomain> <localhost>

- Ensure that the user name used which tomcat is installed has read-write permissions for:

/var/tmp folder – Non Windows operating systems
C:\temp folder – Windows operating system

WebLM Software

Download WebLM software from http://support.avaya.com under the VPNremote phone product listing.

Files:
WebLM_Windows.zip
WebLM_Other.zip
WebLM_Release_Notes.doc

Follow the installation process described in the document named "WebLM_Release_Notes.doc" for both Windows and Non-Windows platforms.

10.3 Configuration

The WebLM URL is configured through the 46vpnsetting.txt file that is provided by the http/TFTP servers. The following is the set command that will configure the VPNremote phones with the URL address for the WebLM license server.

SET NVWEBLMURL http://XX.XX.XX.XX:8080/WebLM/LicenseServer

In this example replace XX.XX.XX.XX with IP address or FQDN of your WebLM server.

Note: The VPNremote phone will contact the license server every 10 minutes after being configured.

Note: VPNremote Phone has a grace period of 30 days, so it will continue to function if the license server is down.

10.4 VPNremote Phone Syslog Messages

The VPNremote phone can be configured to send Syslog messages through the VPN tunnel to a defined Syslog server with the following commands

There are two messages that the user may see at startup
Phone:

(1) VPN License error
Trial period nearing expiry.

This error message implies that the phone has not been able to contact a WebLM server for the past 15 days. This is a warning only message and phone will continue to function normally after 2 minutes.

(2) VPN License error
Trial period expired.

This error message implies that phone has not been able to contact a WebLM server for the past 30 days or could not get a license from the WebLM server. In this case the phone will not attempt to connect with the call server.

If phone is up and running and cannot contact the WebLM server for 15 days or cannot acquire a license after trying for 2 hours, the date and time field on top line will be replaced by following text, "VPN LICENSE ERROR".

Syslog:

VPN License error: WebLM Server no responding
Server is not responding

VPN License error: WebLM Server invalid.
Response from WebLM was invalid

VPN License error: VPN licenses not available, Rebooting
Phone attempted to get a license for 4 hours from WebLM server and WebLM kept refusing to give one, at this point the phone will stop trying, reboot and will block Voice Services.

VPN License error: Phone service is blocked VPN license not available
Cause is the same as above, but after reboot.

VPN License error: VPN licenses not available
Phone sends these messages for 4 hours every 10 minutes before the previous (final) message before rebooting. (Consider this a serious warning)

VPN License error: WebLM URL not configured
If WebLM URL is not configured there will be a Syslog message sent every 10 minutes.

VPN License error: Rebooting trial period expired
Phone has been operational for 30 days without a license.

VPN License error: Phone service is blocked trial period expired

Phone has been operational for 30 days without a license, this message displayed after reboot.

10.5 VPNremote Phone license

When the phone license is purchased, it will be generated through the RFA system. Once generated the license will be emailed to the customer for installation.

To install the license you will log into WebLM using a browser.
http://<ip address/DNS name>:8080/WebLM/index.jsp

Select the option " Install License"
Browse to file location and select license file.
Click "Install"

The license will now be installed and ready for use.

Note: If you are running a WebLM version older than 4.3, you will need a non-enterprise license generated to allow it to be installed.

11 Preparing Communication Manager for VPNremote Phone

From an administrative perspective, the VPNremote Phone is seen as just another extension on Communication Manager. The phone could have a DID or non-DID number and it is designed to behave just like an IP Telephone connected inside the corporate network.

Deploying a VPN Phone really consists of only two main steps. These are 1) administering a new extension and 2) administering access to the VPN network.

Single Extension:
If the end user works remotely full time then a single extension can be configured for an IP Telephone.

Bridged Extension:
When bridged extensions are used, there are actually two phone numbers (DID, non-DID, or combination of the two) but they act as a single phone. When you receive a call, both phones ring. When you have a message, the message waiting light appears on both phones.

One reason to use a bridged extension is when the user has both an office phone and a home office. With bridged extensions, their office phone is a DID number and their VPNremote Phone is a non-DID number and they are bridged together.

Since the VPNremote phones are remotely connecting it is a good idea to place the VPNremote Phone extensions on their own IP Network Region. Due to a wide range of home network ISP bandwidths, a codec setting of G.729 with 3 Frames per Packet is suggested. This allows for a larger range of users to use the service.

CM Levels
Version 3.0 or later

See Reference links for more details.

Security and Avaya Communication Manager Media Servers
http://support.avaya.com/elmodocs2/s8700/docs/Media_Server_Security.pdf

Avaya IP Telephony Implementation Guide for CM3.0
http://support.avaya.com/elmodocs2/comm_mgr/r3/IP_GUIDE_3.0.pdf

IP Telephony Deployment Guide
http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/245600_3_4_1.pdf

Administrator Guide for Communication Manager
http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/03_300509_1.pdf

12 Frequently Asked Question

12.1 How do I know if VPNremote phone will work with my security gateway?

Refer to "Preparing Security Gateway for Remote Access" to see what are the various methods supported by VPNremote Phone for building IPsec tunnels. The table below shows which security gateway has been tested with VPNremote phone. If your security gateway is not in the list below Refer to your security gateway manufacturer provided admin guide to see if security gateway supports Xauth with preshared key. If answer is yes try using one of the predefined 46vpnsetting.txt templates. If none of the predefined templates work contact Avaya Support, some tweaking of the templates might be required to get the VPNremote phone work with your security gateway. Most common reasons are

- Proprietary Xauth extension (For example Nortel).
- Security Gateway expects IPsec clients to use something other than "ID_KEYID" and "ID_USER_FQDN" as IKE ID type.
- Security Gateway cannot handle multiple IKE proposals sent by IPsec clients.
- Security Gateway enforces strict match for IKE and IPsec SA life time.

Manufacturer	Device	Firmware Version
Avaya	SG series	4.6
Avaya	VSU series	3.2

Juniper/Netscreen	NS Series	Screen OS 5.3
Juniper/Netscreen	ISG Series	Screen OS 5.3
Cisco systems Inc	Concentrator 3000 series	4.7

12.2 Does VPNremote phone support authentication using SecureID from RSA?

VPNremote phone has been tested with all the devices listed in previous section using SecureID from RSA. If VPNremote phone does not behave as expected please verify that the manufacturer provide native IPsec client is working as expected before contacting Avaya support. The regular user authentication should always work but there could be issues in new PIN and next token mode. This usually happens when a user enters wrong password multiple times or user is supposed to create/accept server generated pin.

12.3 What are special consideration required when using SecureID from RSA for authenticating VPNremote phone users ?

RSA ACE server can be configured to
Generate a PIN when secureID token is used for the first time and prompt the user to accept the PIN.

OR

Prompt the user to enter a PIN when secureID token is used for the first time.

You should avoid configuring the ACE server to generate a PIN because this will typically require end user to enter 'y' in the password field which is not possible if you have set the password type to 3 (One Time Numeric).

12.4 How is the Preshared Key and Password stored by VPNremote Phones?

There are specific vulnerabilities associated with the Xauth and PSK method of establishing a VPN. The person who has access to the network and knows the PSK can use a person-in-the-middle attack to recover another users personal ID and password. Some organizations may mitigate this vulnerability by keeping the PSK secret from the users of the VPNphones. This can be accomplished by using the procedures in section 8 above away from the end users. When the phone is presented to the end user, the PSK is stored in flash and not available to the user. However, the phone is now a sensitive device so its loss can give away the PSK for all the users of the group. The other method is to make sure all users of a group are equally trusted and they are advised of the consequences of attempting to recover another group member's user ID and password.

12.5 My SOHO router supports QoS, How do I use it for VPNremote phones?

QoS is an IP capability that allows some packets to be flagged as priority packets. Those packets that support Real Time Protocol (RTP) for video and IP telephony are given priority over other packets. Many SOHO gateways support QoS and they each have different methods of signifying a device as getting priority treatment. Refer to the SOHO

gateway manufacturer documentation on how to configure the VPNphone for QoS service.

12.6 Talk path does not establish when calling some extensions?

Make sure you have setup the security gateway as recommended in "Preparing Security Gateway For Remote Access."

12.7 How does the WebLM Server Interact with the VPNphone

The WebLM server is a license server developed by Avaya to enforce licensing for many of its products. When an enterprise purchases VPNphone licenses, the Avaya sales organization creates a license file for the number of VPNphones purchased. As part of the sales process, the enterprise identifies a computer system within the enterprise network as the WebLM server. The enterprise network administrator provides the MAC address of the first network interface on that computer to Avaya and a license is generated that is unique to that server.

The WebLM application is provided as part of the package of software for VPNphone deployment. The WebLM application requires that the computer that it will execute on have Apache as well as Tomcat applications. See section 11 for the installation procedures.

The license management is accomplished during VPN establishment phase of the VPNphone initialization. The VPNphone contacts the WebLM application and registers, thus consuming one license. As the VPNphone is operational and the tunnel is up, the VPNphone contacts the WebLM server every 10 minutes to indicate it is still using the license. If the WebLM server doesn't hear from the VPNphone for 10 minutes, it assumes the phone has a problem and returns the license to the unused pool. When the VPNphone returns to service, it checks out another license.

All this process is separate from the IP telephone process of licensing and registration within the CM. The VPNphone must be licensed with both the CM and WebLM.